7Б

УДК 004.82:007.52

С.В. Блохина, Л.Е. Адамова, Е.Г. Колупаева, Т.С. Потапова, О.О. Варламов
ООО «МИВАР», ЗАО «Учебный центр "Эшелон"», ФГУП НИИ Радио, г. Москва
ovar@narod.ru

Разработка учебных программ с элементами искусственного интеллекта для обучения в области информационной безопасности и защиты персональных данных

В статье показаны особенности создания различных учебных программ с элементами искусственного интеллекта для обучения в области обеспечения информационной безопасности (ИБ) и защиты персональных данных (ЗПДн). В качестве элементов искусственного интеллекта использовались программы типа «УДАВ». Эти программы позволяют описывать сложные предметные области и проводить на них логическую обработку и вычисления необходимых значений.

Введение

Область технической защиты информации очень тесно связана с областью искусственного интеллекта (ИИ), т.к. все самые современные методы ИИ сразу же находят свое применение для организации как атак, так и защиты информации. Более того, методы ИИ можно использовать и для проведения обучения людей.

В настоящее время актуальность обучения в области защиты персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн) обусловлена следующим. Все операторы должны привести свои ИСПДн в соответствии с требованиями закона №152-ФЗ «О персональных данных» от 27 июля 2006 г. не позднее 1 января 2010 года. Количество зарегистрированных операторов ПДн постоянно увеличивается. На момент написания работы их количество превысило 54 тысячи.

Кроме того, актуальность проблемы защиты ПДн обусловлена целым рядом причин – как общемировых: расширение сферы применения компьютеров и т.п., так и специфических российских, например, большим количеством квалифицированных, но бедных технических специалистов или традиционное русское «авось» по отношению к обеспечению любой безопасности.

Целью данной работы является обоснование необходимости создания учебных программ с элементами искусственного интеллекта для обучения в области информационной безопасности и защиты персональных данных.

Уровни обсуждения проблемы защиты ПДн

К проблеме обеспечения безопасности ПДн существует несколько подходов. Прежде всего, необходимо отметить факт существования двух разных уровней обсуждения этой проблемы.

На первом уровне – политико-юридическом – все проблемы являются достаточно новыми, здесь решаются правовые вопросы, ведутся споры о понятиях, сроках и т.д. Например, до сих пор четко не определено, что же такое «персональные данные». Такие же споры ведутся и в отношении других понятий. На наш взгляд, эти споры обусловлены

тем, что информатика продолжает стремительно развиваться и расширять сферу своего применения. Многие понятия, привычные еще вчера, в настоящее время имеют уже совсем другое решение, а через 5 – 10 лет все опять может измениться. Конечно, юристам проще иметь дело с чем-то «застывшим», фиксированным, имеющим долгую историю. Информатика сейчас все делает наоборот: именно свойствами информатики обусловлены правовые сложности и наличие споров и противоречий. В ближайшее время ничего не изменится: юристы не успевают за развитием информатики.

На втором уровне – техническом – проблемы защиты ПДн являются продолжением и «плавным» развитием методов технической защиты информации (ТЗИ) и противодействия техническим разведкам (ПД ТР). По сути, все методы и задачи остались теми же, но изменился только объект защиты. Теперь это «персональные данные». Причем с точки зрения ТЗИ и ПД ТР все равно, что такое ПДн с юридической точки зрения. Отметим, что область ТЗИ и ПД ТР на «западном сленге» называется – «информационная безопасность» (ИБ), хотя эти понятия не совсем равнозначные, но для обычных людей все эти три термина стали синонимами.

Специалистам в области информационной безопасности хорошо известно, что можно защищать любые данные ограниченного доступа, а «персональные данные» – это всего лишь одна из форм таких данных. В зависимости от физической среды и особенностей передачи и/или обработки данных будут применяться уже известные и вновь разработанные методы ТЗИ, ПД ТР и ИБ. Поэтому на техническом уровне обеспечения безопасности ПДн проблем гораздо меньше и имеют они абсолютно другую природу.

Подчеркнем, что новые методы и достижения в области искусственного интеллекта (ИИ) и обработки информации порождают и совершенно новые, порой весьма неожиданные, возможности для создания угроз безопасности ПДн. Если внимательно изучить модель 9 видов технической компьютерной разведки, которая излагалась ранее [1], [2], то можно выявить следующее. Существует как минимум 2 вида компьютерной разведки – семантическая и пользовательская - являются непосредственным следствием применения методов ИИ, а ранее подобные задачи могли решаться только людьми. В настоящее время возможности технических средств по обработке и анализу информации в автоматическом режиме значительно возрастают, благодаря достижениям информатики, а в первую очередь – области ИИ. При обучении все это необходимо предусмотреть. Кроме того, в самом процессе обучения надо применять новые методы и средства ИИ.

Необходимость включения основ представления информации и обзора возможностей и особенностей технической разведки

Опыт обучения безопасности ПДн показывает, что необходимо прежде всего объяснять основы представления информации в виде миварного пространства и вектора-«двойки»: 1) материальный носитель информации и 2) содержание (смысл) информации [1], [2]. Без этого обучаемые не могут понять: как и почему могут проявляться «материальные носители информации» в различных физических средах. Подчеркнем, что применение миварного подхода в обучении является новым элементом и требует отдельного упоминания и обоснования. Именно **миварный подход** наглядно показывает, как связаны носители и смысл информации, а также то, что одинаковые по смыслу сообщения могут иметь абсолютно различную физическую среду – материальный носитель.

Большой интерес у слушателей вызывает и разработанная пространственно-временная модель универсального описания хранения и передачи информации [3]. Эта модель основывается на выделении: отправителя информации, времени передачи и

получателя. Если отправитель и получатель различны, а время передачи мало, то это передача информации. Если отправитель и получатель одинаковы, а время передачи велико, то это хранение информации. Возможны различные варианты, но данная модель очень полезна и удобна для анализа технической разведки. В этом же разделе целесообразно сразу предложить классический подход к определению «канала» технической разведки [4], когда выделяют (вектор-«тройку»):

1) источник информации (объект защиты),

2) среда передачи данных (материального носителя информации),

3) средства добывания информации (приемник материального носителя информации), который и является инструментом ТР.

Наборы таких «троек» образуют различные «технические каналы добывания (“утечки”) информации».

Напомним, что уже сейчас известно более 30 видов ТР по самым разнообразным физическим полям и проявлениям. После рассмотрения процессов передачи и обработки информации, которые могут проявляться опосредованно где угодно и когда угодно на основе всемирного закона «взаимосвязи мира», слушатели понимают особенности передачи и добывания материальных носителей информации. Затем целесообразно продемонстрировать обучаемым на простых примерах процедуры выявления «содержания информации» на основе материальных носителей.

Подчеркнем, что именно описание общей схемы, обзор возможностей и особенностей технической разведки наглядно демонстрирует обучаемым необходимость защиты ПДн на техническом уровне и обязательность построения специальной системы защиты информации (ПДн).

Угрозы, объекты, меры и основные принципы ИБ

На следующем этапе обучения целесообразно рассмотреть угрозы безопасности информации, условия ее использования, защищаемые объекты и их связь с ущербом, субъектами которого всегда являются люди. Особое внимание традиционно необходимо уделить 3 основным свойствам:

1) доступности;
2) целостности;
3) конфиденциальности,

а также двум относительно новым:

4) неотказуемости субъектов от выполненных действий;
5) защите от неправомерного тиражирования.

После завершения обсуждения этих технических аспектов обеспечения безопасности любой информации следует перейти к основным мерам и принципам обеспечения ИБ: правовым, морально-этическим, технологическим, организационным, физическим и техническим.

Удивительно, но для многих слушателей полным откровением является перечисленный порядок важности мер защиты. Почему-то практически все считают, что есть только физические и технические меры защиты. Это заблуждение необходимо обязательно и достаточно подробно объяснить.

Для дальнейшего понимания особенностей защиты ПДн в российских условиях необходимо рассказать слушателям о государственной системе защиты информации в России, ее истории, состоянии и перспективах. Здесь же целесообразно разъяснить основные термины: «лицензирование», «сертификация» и «аттестация».

Если позволяет время обучения, то надо привести виды сертификационных испытаний и заострить внимание слушателей на том, что за специальными сокращениями (например, «АС 1Г») стоит подробное описание таких требований на нескольких страницах текста. Для многих слушателей это также является важным открытием, облегчающим в дальнейшем понимание материала.

Нормативная база по защите персональных данных

Только после указанного выше материала целесообразно переходить непосредственно к нормативной базе и основным понятиям по защите ПДн. Желательно привести конкретные примеры ущерба от нарушения требований по защите ПДн.

Отметим, что традиционно обучение начинают, минуя указанные выше материалы, что создает дополнительные трудности для слушателей. Новизной нашего подхода является именно то, что все обучение надо излагать в указанной последовательности. Наш практический опыт успешного преподавания наглядно доказывает правильность нашего подхода.

Кроме того, традиционно слушателям ничего не рассказывают о новых и перспективных возможностях науки, прежде всего, в области ИИ. Следовательно, сильно уменьшается актуальное время полезности проведенного обучения, т.к. новые возможности ИИ регулярно, как правило, каждые 3 – 5 лет, значительно изменяют возможности как средств нападения, так и средств защиты информации. Считаем необходимым особенно подчеркнуть важность преподавания не только существующих угроз и средств защиты, но также и материала о ближайших перспективах технических средств и методов обработки информации. Например, разработанная с нашим участием программа «УДАВ» наглядно демонстрирует новые возможности ИИ по логической обработке сложных предметных областей в реальном времени и с линейной вычислительной сложностью [2].

Если времени для обучения мало, то надо привести только основные требования: федеральный закон о ПДн, основные положения постановлений Правительства РФ и приказ «трех» по проведению классификации ИСПДн. Необходимо упомянуть, что вводятся типовые и специальные ИСПДн. В типовых – требуется обеспечение только конфиденциальности ПДн, а в специальных – дополнительно требуется обеспечить хотя бы одну из характеристик безопасности ПДн: защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий.

Всего выделено 4 класса типовых ИСПДн: К1 (значительные негативные последствия), К2 (негативные последствия), К3 (незначительные негативные последствия), К4 (отсутствие негативных последствий). Отметим, что на практике структура классификации не очень понятна слушателям. Можно рекомендовать использовать модернизированное описание классов ИСПДн без таблицы, а перечнем классов, указанием последствий и описанием условий отнесения к каждому классу (пример в презентации). Это модернизированное описание выполнено нами и является достаточно новым и интересным материалом.

После изучения классификации целесообразно переходить к обзору документов ФСТЭК России и ФСБ России, в которых изложены конкретные требования, рекомендации, основные мероприятия по обеспечению безопасности ПДн, методики и описания моделей угроз. Степень подробности изучения данных документов очень сильно зависит от запланированного времени обучения. При проведении краткосрочных семинаров и обучений целесообразно дать только краткий обзор.

При этом необходимо помнить, что в настоящее время документы ФСТЭК России относятся к информации ограниченного доступа. К сожалению, непосредственное чтение этих документов весьма затруднительно.

Изучение девяти видов компьютерной разведки

Наш опыт позволяет сделать вывод, что изучение компьютерной разведки и «технических мер по защите от НСД» целесообразно предварять описанием девяти видов компьютерной разведки. Эта модель «9 видов ТКР» [1], [2] позволяет слушателям по существу разобраться в сложной и постоянно развивающейся области компьютерной разведки. Напомним, что по принципам построения программно-аппаратных комплексов, каналам распространения информации и функциональному предназначению выделяют техническую компьютерную разведку, обеспечивающую добывание:

- информации из компьютерных систем и сетей;
- характеристик их программно-аппаратных средств и
- характеристик пользователей,

которая, включает:

1) семантическую,
2) алгоритмическую,
3) вирусную,
4) разграничительную (НСД),
5) сетевую,
6) потоковую,
7) аппаратную,
8) форматную и
9) пользовательскую компьютерные разведки.

Эту модель можно быстро, наглядно и красиво представить на презентации таким образом, что слушатели все хорошо приймут. Конкретные примеры можно подготовить самим или запросить у авторов данной статьи.

Подсистемы обеспечения безопасности и сравнение требований

В следующем разделе обучения следует рассмотреть мероприятия по защите ПДн, которые реализуются в рамках 6 подсистем, среди которых первые 4 хорошо известны по защите конфиденциальной информации, а последние 2 официально добавлены впервые, хотя также применялись и ранее:

1) управления доступом;
2) регистрации и учета;
3) обеспечения целостности;
4) криптографической защиты;
5) антивирусной защиты;
6) обнаружения вторжений.

В документах ФСТЭК России подчеркнуто: должна проводиться сертификация программного обеспечения (ПО) ИСПДн на недекларированные возможности (НДВ). Затем целесообразно провести сравнение требования к средствам защиты для автоматизированных систем (АС) и ИСПДн. Специалистами предложено следующее соотношение: К3 – 1Д; К2 – 1Г; К1 – 1В. Тогда защита ИСПДн К1 аналогична защите государственной тайны, а защита К2 – конфиденциальной информации.

Завершение курса обучения зависит от целей и задач, от выделенных часов и т.п. Целесообразно привести примеры проведения аттестаций ИСПДн, рекомендации по действиям поставщика ПО или изучить основные документы, разрабатываемые в организации для подготовки и проведения аттестации.

В качестве конкретного примера приведем несколько вариантов учебных программ, которые успешно прошли практическую апробацию.

Учебные программы обеспечения безопасности ПДн

Целью обучения в области ИБ может быть повышение квалификации руководителей и специалистов подразделений по защите информации; ИТ-подразделений; служб экономической безопасности; аудиторов и аналитиков по вопросам безопасности ИТ; администраторов информационной безопасности; системных и сетевых администраторов; менеджеров, ответственных за работу с персоналом по вопросам обеспечения информационной безопасности и т.п.

Основная учебная программа курса повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» рассчитана на 72 часа. Она имеет целью обеспечить слушателей теоретическими знаниями и практическими навыками, необходимыми для проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн. Задачи курса – изучить: 1) организационно-правовые основы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных и технической защиты информации; 2) модель технической компьютерной разведки; 3) методы и процедуры выявления угроз безопасности информации на объектах защиты; 4) методы оценки состояния технической защиты персональных данных при их обработке в информационных системах персональных данных; 5) методы и порядок осуществления работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Краткосрочные курсы в области ТЗИ

Отметим, что не у всех есть возможность обучаться 72 часа. Если персонал оператора ИСПДн не прошел специального обучения и не получил допуск к самостоятельной работе, то ему нельзя работать в ИСПДн. В этих случаях кроме основного курса у слушателей существует потребность в краткосрочных обучениях: от 4 до 16 часов. Для удовлетворения этих потребностей можно предложить: 1) обучение пользователей; 2) обучение системных администраторов и 3) обучение администраторов информационной безопасности (АИБ). Например, можно предложить следующие краткосрочные курсы.

Введение в безопасность информационных технологий (базовый курс: 1 день, 8 часов). Формирование представлений об основных принципах создания и функционирования подсистем обеспечения информационной безопасности (ПОИБ). Эффективное взаимодействие по технической защите информации всех подразделений и сотрудников. Организационно-правовые основы технической защиты конфиденциальной информации. Модель технической компьютерной разведки. Обзор методов и особенностей осуществления работ по технической защите конфиденциальной информации. Целевая аудитория: 1) все сотрудники организации, обрабатывающие конфиденциальную информацию; 2) руководители и специалисты IT-подразделений и подразделений технической защиты информации; 3) менеджеры, ответственные за работу с персоналом по вопросам обеспечения информационной безопасности.

Безопасность информационных технологий (углубленный курс: 2 дня, 16 часов). Развитие навыков создания и поддержки функционирования подсистем обеспечения информационной безопасности (ПОИБ). Рациональное распределение функций и эффективное взаимодействие по технической защите информации всех подразделений и сотрудников. Модель технической компьютерной разведки. Методы и процедуры выявления угроз безопасности информации на объектах защиты. Методы и порядок осуществления работ по технической защите конфиденциальной информации. Целевая аудитория: 1) руководители и специалисты IT-подразделений; 2) руководители и специалисты технической защиты информации; 3) начальники служб безопасности, руководители и специалисты служб экономической безопасности; 4) аудиторы и аналитики по вопросам безопасности IT; 5) администраторы информационной безопасности; 6) системные и сетевые администраторы.

Введение в безопасность персональных данных при их обработке в информационных системах (базовый курс: 1 день, 8 часов). Изучение основных требований по технической защите персональных данных (ПДн) в информационных системах персональных данных (ИСПДн). Освоение технологий создания и обеспечения функционирования систем защиты персональных данных (СЗПДн). Мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн. Целевая аудитория: 1) все сотрудники организации, связанные с обработкой персональных данных; 2) руководители и специалисты IT-подразделений и подразделений по технической защите информации; 3) сотрудники кадровых служб и менеджеры, ответственные за обработку персональных данных.

Безопасность персональных данных при их обработке в информационных системах (углубленный курс: 2 дня, 16 часов). Актуализация знаний о создании и обеспечении функционирования систем защиты персональных данных (СЗПДн). Выполнение основных требований по технической защите персональных данных (ПДн) в информационных системах персональных данных (ИСПДн). Оптимальное распределение функций и эффективное взаимодействие по обеспечению безопасности персональных данных всех подразделений и сотрудников. Разработка Модели угроз безопасности ПДн по методике определения актуальных угроз для ИСПДн. Мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн. Целевая аудитория: 1) руководители и специалисты IT-подразделений; 2) руководители и специалисты по обеспечению безопасности персональных данных и технической защиты информации; 3) начальники служб безопасности, руководители и специалисты служб экономической безопасности; 4) аудиторы и аналитики по вопросам ИБ; 5) сотрудники кадровых служб, бухгалтерии; 6) системные и сетевые администраторы.

Администрирование информационной безопасности в электронных архивах, созданных на основе «ЭЛАР Саперион» (базовый курс: 1 – 2 дня, 8 – 16 часов, продолжительность зависит от подготовленности слушателей). Курс обеспечивает получение первичных навыков, необходимых для администрирования ЭА и получения допуска к самостоятельной работе в качестве администратора информационной безопасности электронного архива. Изучаются методы и порядок осуществления работ по технической защите конфиденциальной информации в ЭА. Для прохождения курса необходима предварительная подготовка в области создания электронных архивов, администрирования автоматизированных систем и обеспечения безопасности информационных технологий. Целевая аудитория: 1) администраторы информационной безопасности электронных архивов (АИБ ЭА), созданных на основе «ЭЛАР Саперион»; 2) руководители, системные и сетевые администраторы IT-подразделений; 3) руководители и специалисты ТЗИ; 4) аудиторы и аналитики в области ИБ.

Выводы

Проанализированы особенности создания учебных программ с элементами искусственного интеллекта для обучения в области обеспечения информационной безопасности. Рекомендуется применять программы на основе миварного подхода, например, «УДАВ». Возможности технических разведок постоянно увеличиваются за счет внедрения интеллектуальных систем. Необходимо создавать обучающие системы для защиты информации и персональных данных граждан разных стран, учитывая новые угрозы и своевременно внедряя средства защиты информации. У операторов должны быть обучающие системы и обученные специалисты.

Литература

1. Варламов О.О. О системном подходе к созданию модели компьютерных угроз и ее роли в обеспечении безопасности информации в ключевых системах информационной инфраструктуры / О.О. Варламов // Известия ТРТУ, Тем. выпуск «Информационная безопасность». – 2006. – № 7 (62).
2. Материалы сайта «дтн Варламов О.О.» [Электронный ресурс]. – Режим доступа : www.ovar.narod.ru.
3. Отчет. Концепция развития безопасных информационных технологий: обеспечение защиты информации в проектах информатизации России. – М. : Миннауки РФ, НИИ «Квант», 1992.
4. Меньшаков Ю.К. Защита объектов и информации от технических средств разведки / Ю.К. Меньшаков. – М. : РГГУ, 2002. – 399 с.

С.В. Блохіна, Л.Є. Адамова, Є.Г. Колупаєва, Т.С. Потапова, О.О. Варламов

Розробка навчальних програм з елементами штучного інтелекту для навчання в області інформаційної безпеки і захисту персональних даних

У статті показано особливості створення різних навчальних програм з елементами штучного інтелекту для навчання у сфері гарантування інформаційної безпеки (ІБ) і захисту персональних даних (ЗПДн). Як елементи штучного інтелекту використовувалися програми типу «УДАВ». Ці програми дозволяють описувати складні предметні області і проводити на них логічну обробку і обчислення необхідних значень.

S.V. Blokhina, L.E. Adamova, E.G. Kolupaeva, T.S. Potapova, O.O. Varlamov

Development of Program with Artificial Intellect Features for Education in Information and Personal Data Security

Development of a science and engineering expands opportunities of technical investigations. It is necessary to protect the personal data, constantly taking into account new threats and introducing the certificated means of protection of the information in due time. Experts are necessary for this purpose, they must have special training and must receive the admission to independent work with the personal data. Training should be carried out under curriculums of a safety of the personal data.

Статья поступила в редакцию 31.05.2009.